

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

IN THE MATTER OF THE SEARCH OF:

Six Electronic Devices in the Custody of the
Powhatan Sheriff's Office located at 3880-A Old
Buckingham Rd. Powhatan, VA 23139

Case No. 3:23-sw-196

**AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41
FOR A WARRANT TO SEARCH AND SEIZE**

I, William Lopez, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation (FBI), United States Department of Justice, and have been since May 2018. I am assigned to the Richmond Field Office of the FBI in Richmond, Virginia, and am responsible for conducting investigations pertaining to child exploitation. As part of my duties, I have received training regarding the investigation of federal crimes including crimes against children, human trafficking, civil rights, and public corruption. By virtue of my employment with the FBI, I have performed a variety of investigative tasks including, but not limited to, conducting arrests and executing federal search warrants. As a Special Agent, I am an investigative or law enforcement officer within the meaning of 18 U.S.C. § 2510(7).

2. The facts in this affidavit come from my personal observations and review of records, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

3. This affidavit is submitted in support of a search warrant authorizing the seizure and examination of the following evidence items (hereinafter SUBJECT DEVICES) and/or images of the SUBJECT DEVICES in the custody of the Powhatan Sheriff's Office:

- Samsung S10+ – Evidence Item 1
- Samsung Galaxy SM-G975U – Evidence Item 2
- Motorola Cell Phone – Evidence Item 3
- Samsung Flip Phone – Evidence Item 4
- Samsung Galaxy S6 Edge+ – Evidence Item 5
- Samsung Galaxy S6 Edge+ – Evidence Item 6

The SUBJECT DEVICES to be searched are more particularly described in Attachment A, which is incorporated herein by reference.

4. Based on the facts set forth in this affidavit, there is probable cause to believe that evidence and instrumentalities of violations of 18 U.S.C. § 2251(a), Production of Child Pornography; 18 U.S.C. § 2252A(a)(2), Distribution or Receipt of Child Pornography; and 18 U.S.C. § 2422(b), Attempted Coercion and Enticement are located on the SUBJECT DEVICES described in Attachment A. There is also probable cause to search the SUBJECT DEVICES described in Attachment A for evidence and instrumentalities of these crimes and to seize the items further described in Attachment B.

RELEVANT STATUTORY PROVISIONS

5. **Production of Child Pornography:** 18 U.S.C. § 2251(a) provides that it is unlawful for any person to employ, use, persuade, induce, entice, or coerce any minor to engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct if such person knows or has reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce.

6. **Receipt and Distribution of Child Pornography:** 18 U.S.C. § 2252A(a)(2)(A) and (B) provide that it is unlawful for any person to knowingly receive or distribute a visual depiction

of sexually explicit conduct, if the depiction involved the use of a minor, a computer image of a minor or indistinguishable from that of a minor, or a computer image created, adapted, or modified to appear as an identifiable minor, and in which the depiction was moved in interstate commerce, including by computer, and the person knew that the depiction contained such child pornography.

7. **Attempted Coercion and Enticement of a Minor:** 18 U.S.C. § 2422(b) provides that whoever, using the mail or any facility or means of interstate or foreign commerce, knowingly persuades, induces, entices, or coerces any individual who has not attained the age of 18 years to engage in prostitution or any sexual activity for which any person can be charged with a criminal offense, or attempts to do so, shall be imprisoned not less than 10 years up to life. 18 U.S.C. § 2427 defines sexual activity for which any person can be charged with a criminal offense to include production of child pornography as defined in 18 U.S.C. § 2256(8).

8. **Child pornography or Child abusive material** means any visual depiction, in any format, of sexually explicit conduct where: (A) the production involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital or computer-generated image that is substantially indistinguishable from that of a minor engaged in sexually explicit conduct; or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexual explicit conduct. *See* 18 U.S.C. § 2256(8).

9. **Visual depictions** include undeveloped film and videotape, and data stored on computer disk or by electronic means, which are capable of conversion into a visual image, and data which are capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format. *See* 18 U.S.C. § 2256(5).

10. **Minor** means any person under the age of eighteen years. *See* 18 U.S.C. § 2256(1).

11. **Sexually explicit conduct** means actual or simulated: (i) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or

opposite sex; (ii) bestiality; (iii) masturbation; (iv) sadistic or masochistic abuse; or (v) lascivious exhibition of the genitals or pubic area of any person. *See* 18 U.S.C. § 2256(2).

PROBABLE CAUSE

12. In June 2023, the Powhatan Sheriff's Office received a complaint that a 14-year-old female (hereinafter Minor Victim 1 or MV 1) was speaking to adults online inappropriately. One of the adults of concern was a convicted sex offender in Goochland, Virginia – RICHARD TYSON.

13. On August 24, 2023, law enforcement officers executed a search warrant at TYSON's residence located at 4880 West Grey Fox Circle, Gum Spring, Virginia 23065. Five electronic devices were collected during the search and one device was voluntarily turned over after the search was completed, totaling six electronic devices. These six devices are the SUBJECT DEVICES. TYSON lived with one roommate who advised law enforcement at the time of the search of the residence he only had one cellular device and it was not any of the devices collected by law enforcement.

14. At this time TYSON was charged with failing to register his Snapchat social media account with probation.

15. During the interview pursuant to the search warrant, TYSON admitted to communicating with several minors on various social media platforms. Additionally, TYSON admitted to having a personal relationship with multiple male minors.

16. One of these male minors was Minor Victim 2 (MV 2). In a forensic interview, MV 2 advised that TYSON took nude photos of MV 2. TYSON would frequently ask MV 2 to pose nude in exchange for money, which TYSON put on a debit card so MV 2 could purchase things.

17. Another minor male, Minor Victim 3 (MV 3), a 13-year-old male and friend of MV 2, was also interviewed forensically. MV 3 advised that TYSON took nude photos and videos of

MV 3. TYSON would grab MV 3's legs and position them the way he wanted for the nude photos and videos. This occurred numerous times at numerous locations.

18. On a recorded jail call TYSON advised, "I didn't give them [police] the password for the second S10 plus or the Motorola but I don't think either one of them will be that hard to break into and get stuff off of it and if they can actually take images off of my Gallery I am going to be done. So I probably have 100 counts of child porn because I look at stuff that's underage sometimes, not really bad but like teenagers. It's stupid to keep that shit but who the fuck thought this was going to happen?"

19. In September 2023, detectives from Powhatan and Goochland contacted FBI Richmond and provided documentation for a federal referral of the investigation.

TECHNICAL TERMS

20. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. **Smartphone** is a portable personal computer with a mobile operating system having features useful for mobile or handheld use. Smartphones, which are typically pocket-sized (as opposed to tablets, which are larger in measurement), have become commonplace in modern society in developed nations. While the functionality of smartphones may vary somewhat from model to model, they typically possess most if not all of the following features and capabilities: 1) place and receive voice and video calls; 2) create, send and receive text messages; 3) voice-activated digital assistants (such as Siri, Google Assistant, Alexa, Cortana, or Bixby) designed to enhance the user experience; 4) event calendars; 5) contact lists; 6) media players; 7) video games; 8) GPS navigation; 9) digital camera and digital video camera; and 10) third-party software components commonly referred to as "apps." Smartphones can access the

internet through cellular as well as Wi-Fi (“wireless fidelity”) networks. They typically have a color display with a graphical user interface that covers most of the front surface of the phone and which usually functions as a touchscreen and sometimes additionally as a touch-enabled keyboard.

- b. **Internet:** The internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the internet, connections between devices on the internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- c. **Storage medium:** A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, SIM cards, and other magnetic or optical media.
- d. The terms “records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (“DVDs”), Personal Digital Assistants (“PDAs”), Multi Media Cards (“MMCs”), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

21. As described above and in Attachment B, this application seeks permission to search for records that might be found on the SUBJECT DEVICES, in whatever form they are found. The warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

22. *Probable Cause.* I submit that there is probable cause to believe records will be stored on the SUBJECT DEVICES, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. Depending on a variety of factors, a particular computer could easily not overwrite deleted files with new data for many months, and in certain cases conceivably ever.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or

application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

- d. Similarly, files that have been viewed via the internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

23. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on the SUBJECT DEVICE because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.
- b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This “user attribution” evidence is analogous

to the search for “indicia of occupancy” while executing a search warrant at a residence.

For example, registry information, configuration files, user profiles, e-mail, e-mail address books, “chat,” instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user’s intent.

24. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of SUBJECT DEVICES for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the

warrant. In lieu of removing storage media from the SUBJECT DEVICES, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time at a specific location could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.
- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

25. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

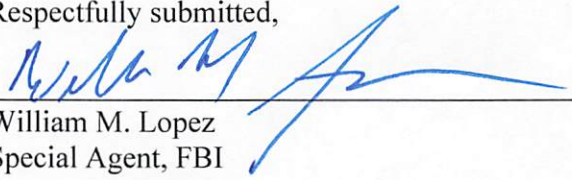
26. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize the execution of the warrant at any time in the day or night.

CONCLUSION

27. Based on the foregoing, I submit that this affidavit supports probable cause for a warrant to seize and search the SUBJECT DEVICES described in Attachment A for evidence and instrumentalities of violations of 18 U.S.C. §§ 2251(a), 2252A, and 2422(b), and to seize the items described in Attachment B.

28. Further, because of the circumstances discussed in the probable cause section of this affidavit, I respectfully request that agents executing this warrant be authorized to seize the SUBJECT DEVICES, and/or images of the SUBJECT DEVICES, which are in the possession of the Powhatan Sheriff's Office.


Respectfully submitted,



William M. Lopez
Special Agent, FBI

Reviewed and approved by AUSA Shea Gibbons

Sworn and attested to me by the Affiant in accordance with the requirements of Fed. R. Crim. P. 41 on November 17, 2023



Hon. Summer L. Speight
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

SUBJECT DEVICES

This warrant applies to the electronic devices, and/or images of the devices, described as follows:

- 1) Samsung S10+ – Evidence Item 1
- 2) Samsung Galaxy SM-G975U – Evidence Item 2
- 3) Motorola Cell Phone – Evidence Item 3
- 4) Samsung Flip Phone – Evidence Item 4
- 5) Samsung Galaxy S6 Edge+ – Evidence Item 5
- 6) Samsung Galaxy S6 Edge+ – Evidence Item 6

which are currently in the possession of the Powhatan Sheriff's Office located at 3880-A Old Buckingham Rd. Powhatan, VA 23139. This warrant authorizes the forensic examination of the devices and/or images of the devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

Particular Things to be Seized

1. All records relating to violations of 18 U.S.C. §§ 2251(a), 2252A, and 2422(b) relating to the production, distribution, receipt, and possession of child pornography and attempted coercion and enticement of a minor:
 - a. Any and all visual depictions of minors;
 - b. Any and all address books, to include names and addresses of minors;
 - c. Any and all contracts, diaries, notebooks, notes, and other records reflecting physical contacts, whether real or imagined, with minors;
 - d. Any and all child erotica, including photographs of children that are not sexually explicit, drawings, sketches, fantasy writings, diaries, and sexual aids;
 - e. Evidence of who used, owned, or controlled the SUBJECT DEVICES at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondences;
 - f. Evidence of software that would allow others to control the SUBJECT DEVICES, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
 - g. Evidence of the lack of such malicious software;
 - h. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the SUBJECT DEVICES.
 - i. Evidence of the times the SUBJECT DEVICES were used;
 - j. Passwords, encryption keys, and other access devices that may be necessary to access the SUBJECT DEVICES;
 - k. Records of or information about Internet Protocol addresses used by the SUBJECT DEVICES;
 - l. Records of, or information about, the SUBJECT DEVICES's internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses;
 - m. Contextual information necessary to understand the evidence described in this attachment.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

If the government identifies seized materials, that are potentially attorney-client privileged or subject to the work product doctrine (“protected materials”), the Prosecution Team will discontinue review until a Filter Team of government attorneys and agents is established. The Prosecution Team will consist of agents, investigators, analysts, attorneys for the government, and personnel designated by an attorney for the government who are involved in the investigation and prosecution of any cases relating to this search warrant. The Filter Team will have no previous or future involvement in the investigation of this matter, and the Filter Team’s work must be overseen and supervised by Richmond Division Assistant U.S. Attorneys. The Filter Team will review all

seized communications and segregate potentially protected materials, i.e. communications to/from an attorney, or that otherwise reference or reflect attorney advice. At no time will the Filter Team advise the Prosecution Team of the substance of any of the potentially protected materials. The Filter Team will seek further guidance from the Magistrate Judge issuing the warrant with respect to obtaining a court order or other authorization before providing any potentially protected materials to the Prosecution Team. After review and subject to the direction of supervising attorneys, the Filter Team then will provide all communications that are not potentially protected materials to the Prosecution Team and the Prosecution Team may resume its review. If the Filter Team decides that any of the potentially protected materials are not protected (e.g., the communication includes a third party or the crime-fraud exception applies), the Filter Team must obtain either agreement from defense counsel/counsel for the privilege holder or a court order before providing these potentially protected materials to the Prosecution Team.